

REMARKS

Claims 1 and 10-13 and 15-19 are pending in the present application, claims 1, 11-13 and 16-19 having been amended and claims 2-9 and 14 having been cancelled without prejudice or disclaimer herein. The Final Office Action and cited references have been considered. Favorable reconsideration is respectfully requested.

Objections

Applicants' drawing was again objected to because it did not include a number as required under §1.84(p) (1). A replacement drawing is attached that shows the words "Figure 1" at the bottom of the page and also includes reference label characters as appropriate.

Furthermore, the specification has been amended as suggested by the Examiner to more accurately describe a method of Applicants' invention and also direct reference to Figure 1 as appropriate.

Withdrawal of these objections is respectfully requested.

Claim Rejections

Claims 1 and 10-19 were rejected under 35 U.S.C. §112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Specifically, claim 1 and its dependant claims were objected to because the naming and referencing to the "possessor(s)" are not consistent. Claim 1 was objected to because the words "each" and "relevant data" had no antecedent basis. Claim 11

was objected to because "the user" and "the operating system" lacked antecedent basis. Claim 12 was objected to because a word was missing between "and memory manager". Claim 13 was objected to because "the functions" lacked antecedent basis. Claims 16–18 were objected to for not being clear. Claim 19 was objected to because the phrase "such as" renders the claim indefinite.

The claims have been amended to overcome these objections. Withdrawal thereof is respectfully requested.

Claim rejections — 35 USC §102

Claims 1, 11-13, 15, 16, 18 and 19 were rejected under 35 U.S.C. §102(b) as being anticipated by Flenley (U.S. Patent No. 6,282,618). Claim 14 was rejected under 35 U.S.C. §103(a) as being unpatentable by Flenley in view of New (U.S. Patent No. 7,353,281) and claim 17 was rejected under 35 U.S.C. §103(a) as being unpatentable by Flenley in view of Malcolm (U.S. Patent No. 7,333,956).¹ These rejections are respectfully traversed for the following reasons.

Claim 1 recites a method for securing by software confinement, a computer system which executes codes which manipulate data, involving at least one memory manager managing memory allocation units, at least one possessor of memory allocation units, and at least one requesters of memory allocation units. The method comprises performing an allocation of memory by the memory manager upon request

from another component of the operating system which transmits to said memory manager, the identity of the requester, performing a check by the memory manager of the whole of the memory allocation units, each memory allocation unit being associated with a possessor of the memory allocation unit, performing an encryption of the data of each possessor by means of a key associated with this possessor, performing a check by the memory manager, for each request to access a memory allocation unit, of the identity of the requester, if this identity is not identical to that of the possessor of the memory allocation unit, then access to the memory allocation unit is refused by the memory manager, and performing, by means of the memory manager, encryption (in the case of a write request) or decryption (in the case of a read request) of the data contained in (in the case of a write request) or requested by (in the case of a read request) the request with the key associated with the possessor, this key being at least recalculated by the memory manager. The memory manager dynamically calculates the key associated with a possessor from a secret associated with the possessor and a master key to which only the memory manager has access. This is not taught, disclosed or made obvious by the prior art of record.

Specifically, to advance prosecution, and without conceding the merits of the rejection, the features of the canceled claim 14, which is not alleged to be anticipated by Flenley, have been added to claim 1. Therefore, the amended claim 1 is not

¹ The Office Action refers to claims 4 and 7 on pages 8 and 9, respectively. Applicant assumes that these are typographical errors and has responded in accordance with that assumption.

anticipated by Flenley. Claims 10-13 and 15-19, being dependant from claim 1, are not, *a fortiori*, disclosed by Flenley.

Claim 1 will be discussed with respect to the rejection under § 103.

As a general remark, Flenley and Applicant's inventions concern different fields — remote database vs. memory allocation. Therefore it would not have been obvious one skilled in the art of memory allocation to apply Flenley's disclosure to Applicant's problem.

Flenley does not disclose nor make obvious several key aspects of claim 1, even following Examiner's interpretation of Applicant's possessors and requesters as Flenley's user.

Applicant's method involves at least one possessor and at least one requester of memory allocation units. It is apparent in claim 1 that possessor and requester are distinct roles involved in different steps of Applicant's method. No such role distinction is taught by Flenley. Flenley's disclosure only explicitly involves a single user of the computer system at any given time. Flenley does not specifically address the confidentiality of information between simultaneous users, only between successive users (Flenley, col. 4, l. 29–34).

Applicant's method comprises a step of "performing an allocation of memory by the memory manager upon request from another component of the operating system which transmits to said memory manager, the identity of the requester". Flenley's disclosure does not involve an applicable concept of identity of the requester, since the requester in Flenley's disclosure is always the user. Flenley discloses using the shared memory controller to store a user's account details (col. 4,

I. 61–66), but the user's identity is data stored using the memory manager, rather than information that influences the behavior of the memory manager as in Applicant's claim. The aforementioned account details may be sent to a separate computer system such as a bank server which will verify said details for its own purposes (col. 4, I. 61–65); this has no bearing on the memory controller. Thus, Flenley does not teach the transmission of the identity of the requester.

Applicant's method comprises a step of "performing a check by the memory manager, for each request to access a memory allocation unit, of the identity of the requester; if this identity is not identical to that of the possessor of said memory allocation unit, then access to the memory allocation unit is refused by the memory manager". As discussed above, Flenley does not disclose an identity of the requester (user). Flenley discloses a check of the identity of the user by a computer system such as a bank server or other web site that is separate from the memory manager and does not participate in the behavior of the memory manager (col. 4, I. 61–65; col. 5, I. 6–9); in particular, Flenley does not teach that a consequence of said check is an access refusal by the memory manager. Furthermore, as seen above, Flenley does not distinguish between a requester and a possessor of memory; such a distinction is fundamental to the step under consideration.

Applicant's method comprises a step of "performing, by means of the memory manager, encryption (in the case of a write request) or decryption (in the case of a read request) of the data contained in (in the case of a write request) or requested by (in the case of a read request) the request with the key associated with the possessor, this key being at least recalculated by the memory manager". Flenley

teaches encryption (col. 4, l. 37–45) and decryption (col. 4, l. 46–48). Flenley teaches that the key is fetched from a key store in volatile memory (col. 4, l. 43–45; col. 4, l. 47–48), said key having been previously entered into said store (col. 4, l. 20–24). Thus Flenley does not teach a recalculation of the key by the memory manager.

The characteristics issued from previous and canceled claim 14 recite that “the memory manager dynamically calculates the key of a possessor from a secret associated with said possessor and a master key to which only the memory manager has access”. Flenley does not teach calculating a key from two secrets, one secret being associated with the possessor and one secret being private to the memory manager.

New teaches combining a plurality of authentication elements to authenticate a user (New, col. 6, l. 4–8). Specifically, New teaches combining publicly available or guessable data such as a hardware tag field (col. 6, l. 16) and user identification (col. 6, l. 27–28) with a secret in the form of a PGP private key (col. 6, l. 30–31). New uses a secret (the private key) to improve the security of a method that would otherwise rely only on public data for security. This is distinct from Applicant's proposal to combine two secrets to improve security.

Furthermore, as all authentication data is stored on the token, an attacker capable of accessing the data on the token would gain access to the whole authentication data required to gain access to the resources protected by the access control mechanism disclosed by New, regardless of how much data was amalgamated to form the authentication data. In contrast, Applicant recites combining a secret associated with a possessor to a master key to which only the memory manager has

access, so that an attacker capable of obtaining the private data of either the possessor or the memory manager, but not both, would not be able to decrypt the data belonging to the possessor.

It would not have been obvious from New's teaching to one skilled in the art to combine two secrets held by different parties to form a secret key. Thus, the subject matter of claim 1 would not have been obvious to one having ordinary skill in the art.

With respect to claim 16, a memory allocation unit according to Applicant's invention corresponds to the space in memory in which a variable's value is stored in Flenley's disclosure. Flenley teaches checking whether the name of a variable is valid (col. 3, l. 61–64). Flenley does not teach checking the integrity of the space in memory in which the value is to be stored.

Moreover, claim 16 must be read in view of claim 1. The subject matter of claim 16 would not have been obvious to one having ordinary skill in the art. As per claims 10-13, 15 and 17-19, they must be read in view of claim 1. Thus, the subject matters of claims 10-13, 15 and 17-19 would not have been obvious to one having ordinary skill in the art.

CONCLUSION

In view of the above remarks, Applicants respectfully request reconsideration and withdrawal of the outstanding rejections of record. Applicant submits that the application is in condition for allowance and early notice to this effect is most earnestly solicited.

Appln. No. 10/540,325
Amdt. dated August 13, 2009
Reply to Final Office Action of April 14, 2009

Atty. Dkt. HAMEAU=1

If the Examiner has any questions, he is invited to contact the undersigned
at (202) 628-5197.

Respectfully submitted,

BROWDY AND NEIMARK, P.L.L.C.
Attorneys for Applicant(s)

By /Ronni S. Jillions/
Ronni S. Jillions
Registration No. 31,979

RSJ:itm
Telephone No.: (202) 628-5197
Facsimile No.: (202) 737-3528
G:\BNM\Mout\HAMEAU1\Pto\2009-08-12AmendmentAF.doc